

Protecting Your Workplace: 10 Anti-Virus Rules

Kaspersky Lab 2001-02-05

Protecting Your Workplace: 10 Anti-Virus Rules

by *Denis Zenkin, Kaspersky Lab*

last updated Feb. 5, 2001

Regardless of how one makes his or her living, computers and the Internet are becoming an increasingly important part of our daily professional lives. When it comes to protection against viruses, worms and Trojans, there is little real difference between the needs of an accountant, an entrepreneur, a tradesman or any other professional working with a computer. No matter what the work, the fact remains viruses and other malicious code can be enormously destructive to the vital information and the computing systems that individuals and businesses rely on for their success.

Despite all the advances in anti-virus technology, malicious code remains a constant threat. Why is this? Because regardless of how well-developed security technologies may become, they are only as effective as the people operating them allow them to be. In the chain of computer security, human error continues to be the weakest link. It can be argued that the most powerful instrument of information security is user behaviour. With that in mind, this article will endeavour to set out ten fundamental rules that will allow users to minimize the threat that viruses, worms and Trojan may pose. When it comes to viruses, there is no such thing as 100% certainty. However, if users learn these fundamental rules, and follow them diligently, they can rest assured that they will as well-protected as possible.

Rule 1: Update your anti-virus program regularly

At this point in time, it should go without saying that all computers should be equipped with anti-virus software; however, computer users should not think that this measure is sufficient in and of itself. Anti-virus scanners are only able to detect and delete a computer virus that is found in its anti-virus database. (There are anti-virus programs that are capable of identifying and deleting recently developed viruses that are not described in the current edition of the anti-virus database. However, even this is not enough to ensure absolute protection from computer viruses.) That is why it is very important to update your anti-virus database regularly. The more often you update the database, the more viruses your anti-virus software will be equipped to detect, and the more securely protected your workplace will be. The best solution is to

update your anti-virus software on a regular basis, either weekly or daily.

Almost all anti-virus vendors provide updates on their web-sites. Some vendors provide several anti-virus updates per day. Therefore, if possible, it is advisable to set your event scheduler (usually supplied with the most contemporary anti-virus programs) to download updates 2 to 3 times per day: in the morning, in the afternoon and in the evening. This will minimize the window of opportunity for newly developed viruses to sneak in unrecognised.

Rule 2: Do not open unexpected attachments

Increasingly, viruses are sent as attachments to e-mails. This is a particularly insidious method of transmission because often people will open attachments that have been sent by acquaintances, co-workers, or friends, only to find that the attachment is in fact a virus. As a result, the best rule for protection is to never open an unexpected attachment. Sadly, this rule even applies to attachments sent by otherwise trusted sources, such as friends and family. Attachments sent by your trusted parties may be infected without their knowledge. More importantly, your acquaintance's computer may have been used by another person without their permission.

Well-known viruses such as LoveLetter, Melissa, etc., replicate themselves to the address book on the infected computer's e-mail program, and send copies of itself to all the e-mail addresses listed there. The messages that these viruses carry contain a text that encourages the reader to execute the attachment. Users should never open attachments with executable files, which carry the .EXE file extension. No less important is the fact that files with "absolutely safe" formats may also contain viruses. If you think that files with the extensions .PIF, .GIF, .TXT cannot carry malware, you are mistaken. Even these formats can hide a virus.

Be absolutely sure that an attachment has been knowingly sent from a trusted source. Do not open any attachment, even from trusted sources, unless it is an attachment that you specifically expect. If you do not expect it, take a moment to confirm with the sender that they did in fact send the attachment and that it is not infected. Better yet, do not execute any attachment until it has been processed by your anti-virus scanner.

Rule 3: Limit the number of people that are authorised to use your computer

Ideally, you should be the only person to use your computer. However, if this is not possible, you should assign limited access rights to others using your computer, clearly defining which operations may be performed by them. This is especially true if people are likely to be using mobile media, such as floppy disks and CDs, in your machine.

Why is this rule necessary? Security is about control. The only way that you can truly control the security of your computer is to know who has been using them, what they have been using them for, and how they have been using them. If you follow each of these ten anti-virus rules, you can be reasonably sure that your risk of infection is acceptably low; however, another user on your computer may not follow the necessary rules of security, in which case, he or she will be placing your computer and your vital information at risk of infection.

Rule 4: Install patches for the software you use in a timely manner

There are viruses that exploit 'holes' or vulnerabilities in operating systems and applications. Anti-virus programs are generally able to protect you from this kind of 'malware' even if you have not installed the appropriate patch for that vulnerability. However, it is still recommended that you visit your software manufacturer's Web site regularly to download and install new patches in a timely fashion. Remember, the less weaknesses that exist in your defences, the more secure your system will be. This rule should especially be applied to Windows and other Microsoft products. This is not to say that these products are necessarily the most vulnerable to computer viruses; rather, we just want to point out that this software is popular not only among users, but among virus-writers as well.

Rule 5: Always scan floppy disks and CDs for viruses before using them

Despite the fact that approximately 85% of all registered cases of computer infection are transmitted through e-mail, we should not ignore the traditional transport for malware: the mobile media (diskettes, compact disks, etc.) Floppy disks and CDs offer an opportunity for viruses to be carried from an infected machine around the defences of another machine, exposing it to subsequent infection. Users should always check these external media for viruses before using it on their computers. It is a simple, straightforward procedure to scan a disk with an anti-virus program. It takes just a few seconds, and can save hours of aggravation.

Compact disks (CD) with pirated software copies are also dangerous. For example, in 1999,

[Kaspersky Labs](#) conducted a test and checked for viruses present in these types of CDs. They found that 23% of the CDs tested were infected.

Rule 6: Be careful with software, even from a credible source

It is not just pirated software that may be infectious. Sometimes even licensed CDs with software from well-established, credible vendors may contain viruses. As well, software downloaded from Internet may carry a virus. You may be certain that the site you are visiting is virus-proof, since a very famous software or hardware company owns it. But it may not be. Sometimes, mistakenly, these sites offer infected software to their visitors. Users may recall the case when Microsoft's site, for several weeks, contained a Word document that was infected with the [macro-virus called Concept](#).

Another source of infection may be a computer that has been taken in for maintenance that may be returned to its owner with a hard drive that is infected with a virus. As a rule, repair shop technicians use the same diskettes to install software and test the hardware of all computers being serviced. In this way, viruses may be transferred from one computer to another. So, if you have just had your computer in for servicing, remember to check it for viruses. In short, cover your back, because even software from credible sources could contain viruses. Remember to check for viruses on this type of software, otherwise, you could lose your valuable data.

Rule 7: Combine various anti-virus technologies

Do not limit your anti-virus protection to an anti-virus scanner, which can be started manually or automatically by the built-in task scheduler. There are a number of other technologies that, if applied in combination with an anti-virus scanner, can ensure the anti-virus protection of your data. These technologies include:

1. Anti-virus monitor: a memory-resident program that checks all your files before they are opened, executed or installed in real time;
2. Integrity checker: checks files, folders and disk sectors for any modification that may indicate a virus infection and informs the user of any such occurrence;
3. Behavioural guard: searches for viruses, not according to their unique code, but according to the sequence of their actions.

A combination of anti-virus technologies as described above can successfully protect your computer against any kind of malware.

Rule 8: Create a virus-free start-up disk for your computer and keep it in a safe place

Sometimes an infected computer cannot be started. This does not mean that a virus has deleted data from your hard drive; it only means that your operating system cannot be loaded any more. To solve this problem, you should use a virus-free start-up diskette containing an anti-virus program that has been developed for your operating system. This diskette will help you to start your computer and delete any viruses in your operating system.

Rule 9: Back up your files regularly

Although this rule will not protect against virus infection, it will allow you to protect your valuable data in case your computer becomes infected (or, as an added bonus, if you have any other problems with your hardware). Whether or not it was a virus that caused your system to malfunction, the only thing that matters is that unless you back up important data, you may lose years of hard work. That is why it is advisable to back up your most valuable data using external media, such as diskettes, MO disks, magnetic tapes, CDs, etc. In this case, whatever might happen, you will always be prepared. (For added protection, the back-up copies should always be stored in a separate location away from the working copy. That way, in case of fire, or other destructive occurrence, the back-up copy will still be safe.)

Rule 10: Do not panic!

We have not set forth these rules in an attempt to convince the reader that computer viruses are unavoidable disasters. Viruses are computer programs, just like the Windows Calculator or NotePad. The only difference is that viruses can replicate themselves, penetrate files computer systems and network resources, causing them to perform tasks as dictated by the virus without a user's permission. Viruses are created by ordinary people and do not have any supernatural attributes. Much more dangerous is your reaction to a virus; i.e., you may panic and make hasty decisions trying to disinfect your computer.

If you believe your computer contains or is infected by a virus, you should do one of the following: if you are a corporate network user, you should immediately contact your network

administrator; if you are working at home, make sure to contact the company that sold you the anti-virus program. You must allow professionals to remedy the problem. After all, that is their job, and it is a service for which you have paid.

Furthermore, as part of a comprehensive information security policy, you should have a pre-established procedure that you can fall back on in case of a suspected infection. This will give you a framework to follow that will minimize the potential for panic and, consequently, minimize the damage that a virus can inflict on your information.

In summary, we would like to reiterate the importance of being cautious when working with a computer. Some may find this to be an exaggeration of the danger; however, in practice, caution is mandatory for the safety of your computer and the vital information that is stored on it. Fortunately, steps can be taken to minimize the risks that are inherent in using computers. While, it would be negligent to suggest that anyone who uses a computer is ever 100% safe from malicious code, by following these ten anti-virus rules, users can protect themselves, as much as possible, against all types of viruses.

[Privacy Statement](#)

Copyright 2006, SecurityFocus